



# ***Cyber Security Program Plan (CSPP)***

---

Template and Guidance  
November 5, 1999

---

**U.S. Department of Energy**  
Office of the Chief Information Officer  
Office of Cyber Security



**Department of Energy**  
Washington, DC 20585

November 5, 1999

MEMORANDUM FOR DIRECTOR, OFFICE OF CIVILIAN RADIOACTIVE  
WASTE MANAGEMENT  
ASSISTANT SECRETARY FOR DEFENSE PROGRAMS  
ASSISTANT SECRETARY FOR ENERGY EFFICIENCY AND  
RENEWABLE ENERGY  
ASSISTANT SECRETARY FOR ENVIRONMENTAL  
MANAGEMENT  
ASSISTANT SECRETARY FOR FOSSIL ENERGY  
DIRECTOR, OFFICE OF NUCLEAR ENERGY  
DIRECTOR, OFFICE OF SCIENCE

FROM:

JOHN M. GILLIGAN *John M. Gilligan*  
CHIEF INFORMATION OFFICER

SUBJECT:

Unclassified Computer Security Program Plan Template

In accordance with Department of Energy Notice (DOE N) 205.1, Unclassified Cyber Security Program, dated 7-26-99, Departmental organizations are required to document cyber security programs by January 26, 2000. An important element of compliance with DOE N 205.1 is the preparation of a Cyber Security Program Plan (CSPP) by each DOE organization.

The attached document includes an annotated template for CSPP preparation. Please take time to review the document and distribute it to appropriate security and information technology professionals within your organization. If you have any questions or comments or require additional copies of the document, please contact Mike Robertson of my staff by phone at 202-586-5837 or e-mail at [mike.robertson@hq.doe.gov](mailto:mike.robertson@hq.doe.gov).

Attachment

# Cyber Security Program Plan (CSPP) Template and Guidance

## Introduction

The Chief Information Officer of the Department of Energy (DOE) provides the following template and guidance for the contents of a Cyber Security Program Plan (CSPP).

## References

- DOE Notice 205.1, Unclassified Cyber Security Program, 7-26-99
- Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources Appendix III, Security of Federal Automated Information Resources
- National Institute for Science and Technology (NIST) Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems, December 1998

## The Cyber Security Program Plan (CSPP) Template

Parenthetical references in *italics* indicate the location of CSPP requirements in DOE N 205.1 and its attached Contractor Requirements Document (CRD).

- I. Environment (*4.u sentence 2; CRD 17 sentence 2*)
  - A. Missions and Objectives (*4.u sentence 2; CRD 17 sentence 2*)
  - B. Operational Concept and Security Environment (*4.u sentence 2; CRD 17 sentence 2*)
  - C. Interoperability Clusters (*4.r sentence 2, 4.u(12); CRD 16 sentence 2, 17.l*)
  - D. Information Flows (if applicable)
- II. Roles and Responsibilities (*4.u(1); CRD 17.a*)
  - A. DOE Manager Identification (*4.u(13)*)
  - B. Individuals or Offices Responsible for Specific Cyber Security Activities
  - C. CSPP Approving Authority (*implicit in 4.u(2), 4.u(3), 4.u(6), 4.u(9); explicit in 4.u(4)(c), 4.u(7)(a), 4.u(8), 4.u(11); CRD 17.a, 17.m*)
- III. Information Systems, Their Interfaces, and Cyber Perimeter Protection Techniques
- IV. Configuration Management (*4.u(3); CRD 17.c*)
- V. Incident, Warning, and Advisory Response (*4.o sentence 1, 4.u(4); CRD 12 sentence 1, 17.d*)
  - A. Incident Response (*4.u(4)(a)*)
  - B. Warning and Advisory Response (*4.u(4)(b)*)
  - C. Incident Response Team Composition (*4.u(4)(c)*)
- VI. Cyber Security Controls (*4.u(6)*)

- A. Authentication (*4.j sentence 2, 4.u(6)(a); CRD 8 sentence 2, 17.f(1)*)
  - B. Access Protection (*4.k sentence 2, 4.u(6)(b); CRD 9, 17.f(2)*)
  - C. Audit (*4.l sentence 2, 4.u(6)(c); CRD 10 sentence 2, 17.f(3)*)
  - D. Security Monitoring (*4.n sentence 3, 4.u(6)(d); CRD 12 sentence 3, 17.f(4)*)
  - E. Malicious Code (*4.q sentence 2, 4.u(9); CRD 15 sentence 2, 17.i*)
  - F. Continuity of Service (*4.m sentence 2, 4.u(6)(e); CRD 11 sentence 2, 17.f(5)*)
  - G. Encryption (if applicable)
  - H. Protection of Classified Information (if applicable) (*4.s*)
  - I. Web Security (if applicable)
  - J. E-Mail (if applicable)
  - K. Data Product Marking (if applicable) (*4.a(2), 4.d*)
- VII. Threat, Risk, and Vulnerability Posture (*4.g(1) sentence 2, 4.u(7); CRD 17.g*)
- A. Responsibilities (*4.u(7)(1); CRD 17.g(1)*)
  - B. Process (*4.u(7)(2); CRD 17.g(2)*)
  - C. Frequency (*4.u(7)(3); CRD 17.g(3)*)
- VIII. Training (*4.o sentence 2, 4.u(8); CRD 14 sentence 2, 17.h*)
- A. Methodology (*4.u(8)*)
  - B. Frequency (*4.u(8)*)
  - C. Participants (*4.u(8)*)
  - D. Responsibilities at Contractor Organization (if applicable) (*4.u(8)*)
- IX. Performance Assessment
- A. Processes and Procedures (*4.g(1) sentence 1, 4.g(2); CRD 5, 17.k*)
  - B. Metrics (*4.u(10); CRD 17.j*)
  - C. Peer Review Process for Contractor Organization (*4.u(11)*)
- X. Plan Change Management (*4.u(5); CRD 17.e*)
- XI. References
- A. Corrective Action Plans (*requirements for such plans are stated in 4.h and CRD 6*)
  - B. Configuration Management Plans
  - C. Continuity of Operations, Contingency, and/or Disaster Recovery Plans
  - D. Memoranda of Agreement
  - E. Related CSPPs
  - F. Related Organizational Security Documents

### **The Cyber Security Program Plan (CSPP) Guidance and Annotated CSPP Template**

If the reference given with topics presented in the template above requires further explanation or if reference is lacking, it is provided below. The annotations seek to avoid repeating information from DOE N 205.1, in particular the definitions and requirements for cyber security controls. The annotations also avoid repeating information in OMB Circular A-130, e.g., the definition of

a major application.

DOE N 205.1 prescribes norms and states requirements for topics to be covered in a CSPP; if a topic is not applicable to a DOE organization, the organization's CSPP is expected to indicate that fact. The template presented above and the annotations to the template that follow constitute informative discussion, amplification, and guidance. Use of this guidance by a DOE organization will speed the review and approval of its CSPP.

DOE N 205.1 requires a CSPP for each DOE organization. A DOE organization can be a DOE contractor, a DOE Headquarters element, or a DOE field element (including a Federal organization). A DOE organization can usually be identified with a site (i.e., a geographic location with a continuous physical perimeter). With the approval of the lead program secretarial officer (LPSO), a DOE organization consisting of multiple sites may prepare a brief organization-wide CSPP as a preamble to a collection of site-specific CSPPs.

A CSPP is one of many plans and other documents that a DOE organization maintains. To reduce paperwork and to facilitate consistency among the body of organizational documents, the CSPP may include by reference information provided elsewhere. The CSPP should have such referenced material attached or should include the information (points of contact, contact information) needed for reviewers to obtain the material.

#### I. Environment (*4.u sentence 2; CRD 17 sentence 2*)

- A. Missions and Objectives. Identify the mission(s) and objectives of the organization.
- B. Operational Concept and Security Environment. Identify the major applications as described in OMB Circular A-130/NIST Special Publication 800-18, general support systems and mission-specific systems used at the organization and describe their relevance and importance to organization missions and objectives. Include security considerations of the environment that may lead to exceptions to the CSPP framework.
- C. Interoperability Clusters. For each Interoperability Cluster used at the organization: identify the cluster by name; identify the protection measures applied to it; identify the person responsible for the overall security of the cluster; and identify the person at the organization who is responsible for the Interoperability Cluster.
- D. Information Flows (if applicable). Describe information flows between information systems within each enclave, between enclaves, within the DOE organization, and between the DOE organization and other organizations (both DOE and non-DOE). Identify security policies (confidentiality, integrity, availability, and accountability) as they apply to different information flows.

#### II. Roles and Responsibilities(*4.u(1); CRD 17.a*)

- A. DOE Manager Identification (*4.u(13)*). Identify, by name and position, the DOE manager who is responsible for the CSPP.
  - B. Individuals or Offices Responsible for Specific Cyber Security Activities (*implicit in 4.u(2), 4.u(3), 4.u(6), 4.u(9); explicit in 4.u(4)(c), 4.u(7)(a), 4.u(8), 4.u(11); CRD 17.a, 17.m*). Identify by name, title, and office other individuals in the DOE organization, or in its contractor or subcontractor organizations, who have major responsibilities associated with the CSPP. Forward pointers may be used to reference later sections of the CSPP in which responsible individuals are identified and their duties with respect to specific cyber security controls described.
  - C. CSPP Approving Authority. Identify the organization and individual responsible for approving the CSPP.
- III. Information Systems, Their Interfaces, and Cyber Perimeter Protection Techniques (*4.u(2); CRD 17.b*). Identify those protection measures taken at each network boundary. Describe techniques and procedures for monitoring intrusion detection systems, or provide a forward pointer to VI.D.
- IV. Configuration Management (CM) (*4.u(3); CRD 17.c*).
- A. Configuration Management and Security. Describe how the organization's CM program establishes and preserves security. In particular, describe how security is tested or demonstrated. Identify organizational requirements for standard configurations throughout the organization, site, Interoperability Cluster, or instance of a major application. Identify organizational processes and procedures for ensuring compliance with standard configurations and for managing exceptions. If the organization CM plan provides information required for the CSPP, this section of the CSPP may reference that plan and include pointers to its security-relevant sections.
  - B. Life Cycle Management (if applicable). Describe how the organization establishes and preserves security throughout the life cycle, including the life cycle phases of: initiation, development/acquisition, implementation, operation/maintenance, upgrade, and disposal. In particular, describe how security is tested or demonstrated in each phase. If the organization has a life cycle management plan that provides the information required for the CSPP, this section of the CSPP may consist of a reference to that plan and pointers to its security-relevant sections.
- V. Incident, Warning and Advisory Response (*4.o sentence 1, 4.u.(4); CRD 12 sentence 1, 17.d*).
- A. Incident Response. Describe how the organization performs cyber security incident

reporting and response. Provide sufficient detail that reviewers can determine how well the organization provides for the protection of not only locally managed resources but also resources of other organizations that may be effected by the incident. Identify degrees of notification and response and the corresponding levels of risk that entail them. Identify variations, if any, in procedures and policies specific to a site, Interoperability Cluster, system, or instance of a major application. Provide references to Memoranda of Agreement with organizations (DOE and non-DOE) responsible for implementing this activity.

- B. Warning and Advisory Response. Describe how the organization handles cyber security warnings and advisories. Identify degrees of notification and response and the corresponding levels of risk. Identify variations, if any, in procedures and policies specific to a site, Interoperability Cluster, system, or instance of a major application.
  - C. Incident Response Team Composition. Identify by role, office, and name (if applicable) members the DOE organization's incident response team, both core (i.e., participating in all responses to incidents) and ancillary (i.e., participating in responses to incidents that affect resources for which they are responsible or that require their specific expertise).
  - D. Release of Public Information (if applicable). Identify organizational policies and procedures regarding the release of information about cyber security incidents to the general public.
- VI. Cyber Security Controls (*4.u(6)*). The following applies to all subsections: Describe the controls applied to the DOE organization's cyber systems. Include (by reference to other organizational plans or policies, if appropriate) non-technical controls (e.g., physical, procedural, personnel) as well as technical controls. Describe how each control conforms to the requirements of DOE N 205.1. Describe how each control conforms to other cyber security Notices, requirements for protection of non-DOE information, and requirements for protection of specific categories of unclassified information, as appropriate. Describe organizational processes and procedures for ensuring the effective application of technical controls. Identify roles, individuals, and offices responsible for implementing, administering, maintaining, using, and testing the correctness of cyber security controls.
- A. Authentication (*4.j sentence 2, 4.u(6)(a); CRD 8 sentence 2, 17.f(1)*) .
  - B. Access Protection (*4.k sentence 2, 4.u(6)(b); CRD 9, 17.f(2)*).
  - C. Audit (*4.l sentence 2, 4.u(6)(c); CRD 10 sentence 2, 17.f(3)*).
  - D. Security Monitoring (*4.n sentence 3, 4.u(6)(d); CRD 12 sentence 3, 17.f(4)*). If

appropriate, cross-reference this section with section V.A, Incident Response.

- E. Malicious Code (*4.q sentence 2, 4.u(9); CRD 15 sentence 2, 17.*).
- F. Continuity of Service (*4.m sentence 2, 4.u(6)(e); CRD 11 sentence 2, 17.f(5)*).  
Identify systems, enclaves, missions, major applications, and/or environments under the DOE organization's authority that require an assured level of availability. For such entities, either describe the continuity-of-service plan or provide references to the DOE organization's relevant plans (e.g., disaster recovery plan, contingency plan, Y2K contingency plan), ensuring that the references are sufficiently detailed to locate information about cyber continuity of service and about continuity of service despite cyber attack. Describe (directly or by reference) the linkages between the continuity-of-service plan and the Security Advisory Handling and Computer Security Incident Reporting Directive. Provide references to Memoranda of Agreement with organizations (DOE and non-DOE) responsible for implementing the continuity-of-service plan.
- G. Encryption (if applicable). If the DOE organization uses encryption to protect information, describe the organizational policies regarding the use of encryption (e.g., key length, key escrow, use of domestic *vice* foreign-developed encryption products, situations in which plaintext information must be available to administrators or investigators), the encryption mechanism(s), the resources protected (e.g., e-mail, data files on laptops), and organizational processes and procedures for key management and for verifying compliance with organizational policies.
- H. Protection of Classified Information (*4.s*) (if applicable). If any of the DOE organization's unclassified systems are located in the same proximate physical environment as a classified information system, describe the controls applied to prevent the transfer of classified information to an unclassified system.
- I. Web Security (*implicitly addressed by 4.u(2), 4.u(6)*) (if applicable). If the DOE organization allows access to the Internet, describe organizational policies restricting use and/or disclosure of information; describe organizational procedures and technical controls for ensuring compliance with those policies. If the DOE organization maintains an externally-accessible Web server, describe organizational policies regarding restrictions on the information placed on and/or collected by the server, the integrity of the information, and the availability of the server; describe organizational procedures and technical controls for ensuring compliance with those policies. If these descriptions are included in III, refer to that section.
- J. E-Mail (*implicitly addressed by 4.u(2), 4.u(6)*) (if applicable). Describe organizational policies regarding confidentiality, accountability, and appropriate use of electronic

mail. Describe organizational procedures and technical controls (e.g., digital signature for accountability, dirty word screening for confidentiality or appropriate use) for ensuring compliance with those policies.

- K. Data Product Marking (4.a(2), 4.d) (if applicable). Describe organizational policies and controls regarding marking data products (e.g., hardcopy, removable media, displays). Describe how each control conforms to requirements for protection of non-DOE information and/or requirements for protection of specific categories of unclassified information, as appropriate.

## VII. Threat, Risk, and Vulnerability Posture

- A. Responsibilities (4.u(7)(1); CRD 17.g(1)).
- B. Process (4.u(7)(2); CRD 17.g(2)).
- C. Frequency (4.u(7)(3); CRD 17.g(3)).

## VIII. Training (4.o sentence 2, 4.u(8); CRD 14 sentence 2, 17.h).

- A. Methodology (4.u(8)).
- B. Frequency (4.u(8)).
- C. Participants (4.u(8)).
- D. Responsibilities at Contractor Organization (if applicable) (4.u(8)).

## IX. Performance Assessment.

- A. Processes and Procedures (4.g(1) sentence 1, 4.g(2); CRD 5, 17.k).
- B. Metrics (4.u(10); CRD 17.j).
- C. Peer Review Process for Contractor Organization (if applicable) (4.u(11)).

- X. Plan Change Management (4.u(5); CRD 17.e). Identify circumstances that would require rewriting the CSPP more frequently than once every 2 years.

- XI. References (if applicable). Attach referenced material or provide information (points of contact, contact information) to enable reviewers to obtain the referenced material.
  - A. Corrective Action Plans (requirements for such plans are stated in 4.h and CRD 6).
  - B. Configuration Management and Life Cycle Management Plans.

- C. Continuity of Operations, Contingency, and/or Disaster Recovery Plans .
- D. Memoranda of Agreement
- E. Related CSPPs. If the CSPP is for a major application, or for a DOE organization at which a major application runs, cross-reference the relevant CSPPs, identify which CSPP takes precedence in case of inconsistency, and identify the individual or office responsible for resolving conflicts.

Identify CSPPs for other DOE organizations with which the DOE organization interfaces electronically. Describe how the organization's CSPP takes into account the potential impacts of the organization's cyber security program on those other organizations. Describe how the organization's CSPP takes into account the potential impacts of other organizations' cyber security programs on its program. Identify processes for detecting and resolving inconsistencies among CSPPs.

- F. Related Organizational Security Documents. Identify such documents as the DOE organization uses to state policy and/or define processes and procedural controls for non-cyber security, that affect the security of cyber systems. These are expected to include physical security, personnel security, protection of special categories of unclassified information, and control of information disseminated to the general public.